International Comparative Legal Guides

Data Protection 2020

A practical cross-border insight into data protection law

Seventh Edition

Featuring contributions from:

Addison Bright Sloane
Anderson Mōri & Tomotsune
Chandler MHM Limited
Clyde & Co
DDPV Studio Legale
Deloitte Kosova Shpk
Deloitte Legal Shpk
D'LIGHT Law Group
DQ Advocates Limited
Drew & Napier LLC
Elzaburu S.L.P.
FABIAN PRIVACY LEGAL GmbH
Herbst Kinsky Rechtsanwälte GmbH
Homburger AG
Khaitan & Co LLP
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys-at-Law
Leśniewski Borkiewicz & Partners
LPS L@w
LYDIAN
Marval O'Farrell Mairal
Matheson
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
NEOVIAQ IP/ICT
Nyman Gibson Miralis
OLIVARES
Pellon de Lima Advogados
PPM Attorneys
Rothwell Figg
Semenov&Pevzner
SEOR Law Firm
SKW Schwarz Rechtsanwälte
SSEK Indonesian Legal Consultants
S. U. Khan Associates Corporate & Legal Consultants
Synch Advokatpartnerselskab
Templars
White & Case LLP
White & Case, s.r.o., advokátní kancelář
Wikborg Rein Advokatfirma AS

ICLG.com

Expert Chapters

Q&A Chapters

Q&A Chapters Continued

Privacy By Design in Digital Health

FABIAN PRIVACY LEGAL GmbH

Daniela Fábián Masoch

1 Introduction

The exponential growth of digital health solutions and products, such as software or internet-enabled devices, brings a range of benefits for patients, the health industry and the general public, from preventing new diseases, monitoring patient conditions, data analysis and personalised medicine, to reducing health costs through more efficient processes.

To be effective, these technologies rely on the use of large amounts of data. Particular caution is needed when personal data are involved, as the processing of personal data – in particular, health-related data – can pose significant risks to the privacy of data subjects and the security of personal data. It is therefore of utmost importance to implement the fundamental data protection principles as laid down in data protection laws, such as the European Union ("**EU**") General Data Protection Regulation (EU) 2016/679 of 27 April 2016 ("**GDPR**"), the EU directive on privacy and electronic communications (Directive 2002/58/EC of 12 July 2002) and applicable national data protection laws. In particular, principles such as data minimisation and transparency, as well as technical security measures like pseudonymisation or encryption, must be embedded in the design, development and use of such solutions. In short: privacy by design ("**PbD**") must be implemented.

With the outbreak of COVID-19 and the efforts to find fast digital solutions to contain the spread of the virus – in particular, through so-called contact-tracing apps, which should help to efficiently interrupt chains of infection – the importance of PbD has increased, as has awareness of the concept. For such apps to be successful and effective, they must be designed in such a way that the privacy of the individual and the protection of his or her personal data are guaranteed, at least in Europe. People must be assured that they are in control of their data, that their data are secure and only used for well-defined purposes, and that their privacy rights are respected. Public trust and acceptance are of paramount importance to encourage the use of such applications where their use is voluntary.

In order to realise the benefits of digital health solutions, those responsible for the development and management of such solutions and data processing, such as healthcare companies or public authorities, must meet the expectations of individuals, gain and maintain their trust, and respect their privacy. PbD has become a critical factor in building and maintaining trust, competitiveness and success in the marketplace.

The challenge is to find the right balance between the potential of digital health to improve health services on the one hand, and the protection of the personal rights of patients and consumers on the other. All legitimate interests and objectives, including data protection, should be taken into account without unnecessary compromise. This approach requires creative solutions in technical and organisational respects.

This article examines the privacy aspects under the GDPR that need to be taken into account when designing digital health solutions, and why this is important to fully exploit the potential of digital health. It also attempts to clarify the concept of PbD and to translate legal requirements into practical solutions, with a focus on mobile applications in the context of digital health.

2 Emerging Digital Health Technologies

Digital health refers to the use of information and communication technologies ("**ICT**") to improve the quality, efficiency, and management of healthcare. Examples of digital health technologies include: telemedicine, health monitoring and care with robots and sensors; wearables, i.e. mobile sensors worn directly on the body that record and analyse physiological data such as blood pressure, temperature, pulse or blood sugar levels in real time; and more generally the Internet of Things ("**IoT**"), i.e. the networking of physical devices equipped with software, sensors and network connectivity to collect and exchange data. Another example is the contact-tracing apps mentioned above, which are highly topical at the time of writing, and which are being developed by various countries worldwide to combat the spread of COVID-19. These apps are designed to alert people who have been in proximity to an infected person for a certain period of time so that they can take appropriate action.

3 The Concept of Privacy By Design

The concept of PbD is a fundamental prerequisite for the effective implementation of data protection. In essence, PbD requires that controllers take into account the principles and requirements of data protection both in the design phase of systems, processes, products or services and throughout the life cycle of personal data; and that they provide for appropriate technical and organisational measures ("**TOMs**") to implement the data protection requirements and to protect the rights of data subjects. Controllers are required to be proactive and anticipate potential privacy-invasive events before they materialise. Privacy by default is a fundamental element of PbD. It requires the controller to implement appropriate TOMs to ensure that, by default, only personal data necessary for each specific purpose of processing are processed. PbD must be implemented in relation to the quantity of data collected, the scope of their processing, the period of their storage, and their accessibility.

While the concept of PbD as good practice has long existed, it was introduced as a legal obligation in Art. 25 GDPR, with substantial fines in case of failure. With this, the legislator wanted to emphasise that it is not enough to set standards, but that these

standards must be implemented in an effective and verifiable manner. However, Art. 25 GDPR does not specify how this obligation should be implemented in practice.

The implementation of PbD requires an assessment of the organisational, process, or product-related risks as well as the privacy risks for data subjects. This assessment aims to determine the necessary measures to be integrated from the outset as part of these products, systems or processes to meet data protection requirements and to protect the privacy of data subjects. Risks may include, for example, excessive collection and disclosure of personal data, processing beyond the initial purpose, unlawful processing, loss, destruction or alteration of data. Such risk assessment, coupled with a conformity assessment, is required for any processing of personal data, regardless of the sensitivity of the data.

Only if the processing is likely to present a high risk to the rights and freedoms of the data subjects, must the controller carry out a data protection impact assessment ("**DPIA**") according to Art. 35 GDPR. A DPIA is a more comprehensive assessment that goes beyond a conformity assessment by assessing the remaining risks to individuals, taking into account the TOMs embedded in the design of the product, system or process. If the residual risk is still considered to be high, the controller must take further risk mitigation measures or, if this is not possible, refrain from processing or consult the data protection authorities. A DPIA will regularly be required for digital health solutions where health-related data or other special categories of data are processed, or technologies are used that may involve new forms of data collection and use.

4 Implementing Privacy By Design in Practice

Legal responsibility for implementing privacy by design

According to Art. 25 GDPR, the controller must implement the concept of PbD. Manufacturers, developers and service providers that are not controllers are only encouraged in Recital 78 GDPR to take into account PbD when developing, designing, selecting and using applications, services and products based on the processing of personal data, and to ensure that controllers and processors can comply with their data protection obligations. In practice, manufacturers of intelligent devices and health application developers will have a keen interest in fully implementing the concept of PbD, in order to remain competitive.

Requirements on the controller

The controller must establish technical measures; for example, pseudonymisation, access authorisations and restrictions, user authentication, encryption, logging, securing system configurations, protection measures against malware and data loss, and physical protection measures.

Furthermore, the controller must take organisational measures that are necessary for the smooth functioning of data protection management. These measures may include, for example, the allocation of responsibilities for the effective implementation of data privacy requirements, the implementation of enforceable policies and procedures for handling and documenting data breaches and data subject access requests, risk management, third-party management, data transfer governance, documentation of processing activities, training and controls. Also, the controller must take appropriate measures to respond to a withdrawal of consent, or to a request for rectification or erasure of personal data or the portability of data.

Technical and organisational measures

The TOMs must be adequate and appropriate to:

- effectively implement data protection principles, such as data minimisation, lawfulness, transparency, confidentiality, purpose limitation, data integrity, storage duration, security, as well as the requirements concerning commissioned data processing and cross-border data transfers;
- integrate the necessary safeguards into the processing to meet the requirements of the GDPR; and
- protect the rights of data subjects.

A measure is adequate if it takes into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons posed by the processing.

Timeline for implementation

The controller must implement TOMs both at the time of determining the means of processing and during the processing itself.

Data protection considerations for digital health solutions

First, it must be determined which laws and regulations are applicable; in particular, whether the GDPR is applicable. It should also be examined whether sector-specific codes of conduct, certification systems, regulatory decisions or guidelines for the development of digital health products are applicable. Ethical considerations should also be taken into account.

Second, it is necessary to determine: which parties are involved in the development, deployment and use of the product, and the respective roles of these parties; who is the controller (several parties may be joint controllers); and, where appropriate, who is a processor. The identification of the controller, i.e. the party which alone or jointly with others determines the means and purposes of the data processing, is essential to determine who is responsible and accountable for complying with data protection requirements under the GDPR.

The following section explains which data protection principles must be observed and how they can be implemented in practice, with a focus on the use of mobile health apps.

Proportionality and data minimisation

Personal data must be adequate, relevant, and limited to what is necessary for the purposes for which they are processed. This means that apps and devices that store or process personal data should be set up in such a way that only the data necessary for the respective purpose or the proper functioning of the app or device are stored and processed.

Personal data are defined as any information relating to an identified or identifiable natural person. In the context of a mobile application, data relating to the device, such as location data or usage data, are also considered personal data. Pseudonymised data, meaning data that are processed in such a way that they can no longer be attributed to a specific data subject without the use of additional information that is kept separately and securely, are also classified as personal data. Only irreversibly anonymised data are not considered personal data and are therefore not subject to the GDPR (and other data protection laws).

The principle of data minimisation can be achieved in different ways; for example, by reducing the amount of personal data or by making it more difficult or impossible to assign the data to an individual.

The type and amount of data necessary for the identified purpose may vary depending on the area of application of the product. If, for example, an app is only used for information purposes, the collection of personal data is usually not necessary or pseudonymised login data might be sufficient. However, if an app is for monitoring health and, if necessary, interacting with a doctor or other persons, considerably more data, especially identification and health data, may be required. In the case of a COVID-19 contact-tracing application, proximity data collected using Bluetooth technology should be sufficient. Location data that can be used to track individuals are not necessary for this purpose, nor are other personal data. Anonymised or at least pseudonymised data should be sufficient.

Depending on the functionalities of the app and the purpose of processing, it must, therefore, be evaluated for each dataset whether the data are necessary to fulfil the purpose or whether the purpose can be fulfilled with less data (reduction of the data volume) or pseudonymised/anonymised data (making identification more difficult or impossible). A distinction should also be made between mandatory and voluntary data, which can be provided additionally to use specific functionalities.

Further measures to minimise data can consist in preventing the linking of personal data collected via the product with personal data stored in other systems unless such linking is necessary for the purpose. Location data should not be collected and stored if a generic location area is sufficient for the application's functionality.

A central question is also where the data should be stored – i.e. only on the user's terminal device or on a central server – and who should have access to the data. If the data are only stored on the mobile device, the user has full control over the data and access. However, if the data are stored on a central server, other people can have access, over which the user has no control. This question is currently being hotly debated in connection with the development of a COVID-19 tracing app, where the proponents of a decentralised solution believe that this approach is more consistent with the principle of data minimisation.

Which approach is ultimately chosen depends on the type of mobile health app and its purposes. With both models, appropriate TOMs must be taken to protect the data from unauthorised access and misuse.

Legal justification

The processing of personal data must be lawful and carried out in good faith, and must have a legal basis, as set out in Art. 6 and 9 GDPR and the ePrivacy Directive. The ePrivacy Directive requires the user's consent for the storage of information or access to stored data on the user's equipment unless the storage and access are legally permitted under national law, or the storage and access are strictly necessary to provide a service explicitly requested by the user. Consent is also required for the use of non-essential cookies or similar technologies on users' equipment, and for the processing of location data other than traffic data, provided that such data are not anonymised.

In health or medical applications collecting and processing special categories of a patient or consumer data, the processing of these data will regularly require the explicit consent of the data subject. Consent must be voluntary and specific to each functionality that serves a distinct purpose. Consent must be based on prior information and, in the case of special categories of data, the use of cookies or location data, consent must be given explicitly and therefore through positive action, such as downloading the application and ticking a consent box. Also, controllers must have a procedure in place which, on the one hand, allows for easy withdrawal of consent and, on the other hand, ensures that in the event of withdrawal, the data collected will not be further processed.

Transparency

Personal data must be processed transparently. A comprehensive privacy notice about what personal data are processed, how they are processed and what they are used for, as described in Art. 12-14 GDPR, must be made available to the data subjects before their data are processed. This notice must, if applicable, also contain information on the use of cookies or similar technology on the terminal equipment and location data, as well as methods for refusing to store such cookies or giving consent to the use of cookies and location data.

Data subjects should have full transparency and control over the processing of their data and understand what data are processed, why, by whom, where and for how long, and how they can exercise their privacy rights.

The privacy notice should be easily accessible to data subjects at any time, before the collection of personal data and throughout the processing, either within the device or through a link to a website. The notice should be easy to understand – where appropriate, in different languages – and have a multi-layered structure in which the essential information is summarised in a first layer, possibly supported visually by symbols, and with further details in a second layer if the user wishes to know more. The product should also allow for changes to the privacy notice and should allow users to manage their profiles and update their privacy settings.

Confidentiality and access to personal data

Personal data must be kept strictly confidential and may only be provided or disclosed to individuals on a need-to-know basis to fulfil the legitimate purposes for which the information was collected.

It is essential to determine whether access to the data by persons other than the user – such as doctors, service providers, insurance companies or authorities – is necessary to fulfil the purposes for which the data are processed. Instances of access to the data, devices, server and network should be documented.

Among the key issues are: Can the user influence and manage his/her access directly through the product? Who enters the data – only the user of the product or other persons, such as a doctor or a pharmacist? Are any service providers involved in the storage or other processing of the data? How is access to or sharing of the data secured? Are the data encrypted during transmission and in storage? Who should have access to what personal data and for what purposes? Are these persons obliged to maintain confidentiality? How is access controlled and restricted?

Purpose limitation

Personal data must be collected only for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes.

The purpose of the processing should be specific and explicit and communicated to data subjects at the time of collection. The functionalities of the app should be set up as such that personal data are only processed for the specific purpose that was identified. Access to servers should be limited to persons that are committed to processing the data for the specified purpose only. If the personal data are to be used for purposes other than those notified, the data should be made anonymous, unless there is another legal basis for this secondary use. In any case, the data subjects should be informed and, unless there is no other legal basis, their consent should be obtained.

Data quality
Personal data stored must be accurate and, where necessary, up to date; every reasonable step must be taken to ensure that inaccurate personal data are deleted or rectified without delay.

The controller must have mechanisms in place to ensure that the data are accurate at the time of collection and are not unlawfully modified after that. There must be a mechanism to correct or delete inaccurate data, possibly by the user of the application.

Data retention
Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, unless regulatory or legal requirements require a longer or shorter retention period.

The controller must define a retention period for each dataset, based on the purpose of the processing and, where appropriate, legal and regulatory retention periods. Mechanisms, including automatic solutions, where appropriate, and responsibilities for the effective erasure of the data, must also be specified. If the data cannot be deleted, they should be made anonymous or, if this is not possible, pseudonymous.

Among the key issues are: Does the product allow for flexible data retention periods? Does the product enable the anonymisation or deletion of data that is no longer needed? Are the data automatically deleted or anonymised after the retention period has expired? Is the data controller notified in advance by the system? Can users delete the data, and if so, how (e.g., by deactivating the app used)? Is there a retention and deletion concept?

Data security
Personal data must be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate TOMs. Such measures should encompass integrity and confidentiality, availability, resilience and traceability, and ensure a level of security appropriate to the risk.

Appropriate control access mechanisms and authentication measures should be embedded in the product infrastructure to detect and monitor unauthorised access to the data. Personal data should be encrypted on the device and, if stored on a server or shared with third parties, in transit and storage. Special attention is required if the data are stored in the cloud.

Privacy rights
Data subjects have a variety of privacy rights, including the right to: information; access, rectification and erasure; restriction of processing; data portability; and objection to automated individual decision-making. They also have the right to complain to their supervisory authority if they feel that their rights are infringed, or their data are not appropriately protected. A process must be in place to respond to data subjects' access requests and other privacy rights.

Among the key issues are: How can data subjects effectively exercise their rights? Does the product allow data subjects to exercise their rights directly through the app; in particular, the right to access their data and correct it in case of inaccuracies or to delete the data from the mobile device by deleting the app? Are any rights restricted? How are rights such as data portability, deletion, or withdrawal of consent guaranteed?

Data processing by third parties and cross-border data transfers
Depending on the roles of the contributors in the development, management and use of the app and the data processed, appropriate contractual obligations must be established to ensure data protection.

The controller must carry out a prior assessment of all data processors to ensure that they implement appropriate TOMs to ensure compliance with the data protection requirements and data subjects' privacy rights.

If personal data are to be transferred to third parties outside the European Economic Area ("**EEA**") in a country without a formal adequacy decision from the European Commission, adequate safeguards, such as EU standard contractual clauses, must be implemented to legitimise cross-border data transfers, unless a derogation as listed in Art. 49 GDPR applies, such as the explicit consent of the data subject.

For any cross-border data flow, the legal basis for such a transfer must be determined, and the necessary steps taken.

Accountability
The controller is responsible for ensuring compliance with the data protection principles and for providing proof of compliance with them. Appropriate processes, regular risk assessments, documentation and reviews of the processing should be in place to support this obligation.

5 Conclusion

To fully exploit the benefits of digital health solutions and ensure their effectiveness, it is essential to embed fundamental data protection principles in the design of these solutions, taking into account organisational, process and product-related risks, as well as risks to the rights of data subjects.

Privacy by design is not only required by the GDPR, and partly by laws of other countries outside the EEA, but is a prerequisite for the effective and sustainable implementation of data protection, the basis for the smooth functioning of data protection management, and a critical factor in achieving the necessary trust of the public, patients and consumers, public authorities, business partners and other stakeholders in such technologies.

Daniela Fábián Masoch is the founder and executive director of FABIAN PRIVACY LEGAL, a law firm specialised in international, European and Swiss data protection laws, governance, risk management and programme implementation. Daniela is a Swiss attorney at law, certified Privacy Professional and ISMS 27001 Lead Auditor, with 30 years of experience in data protection, labour law, risk and programme management, security and related matters. She advises multinational companies from various industries but with a particular focus on the life sciences, pharma and medical devices sector, in the EU, Switzerland and the US, on privacy and data protection issues. Daniela supports her clients in evaluating, developing, implementing and monitoring data protection strategies, governance models and global privacy programmes as well as data transfer mechanisms with a pragmatic approach.
Before commencing her own business in 2015, Daniela held various positions at Novartis, including Global Head Data Privacy, where she was responsible for setting the Group's strategic direction on privacy and for building, implementing and overseeing the global privacy function, global privacy management programme and binding corporate rules.

FABIAN PRIVACY LEGAL GmbH
Bäumleingasse 10
4051 Basel
Switzerland

Tel: +41 61 544 44 01
Email: daniela.fabian@privacylegal.ch
URL: www.privacylegal.ch

FABIAN PRIVACY LEGAL is a boutique law firm specialising in international, EU and Swiss privacy laws and related matters, privacy policies, risk management, programme implementation and maturity level assessments. Our strengths are the combination of expert knowledge and practical in-house experience, an excellent network with industry groups and data protection associations, and close cooperation with experts from a variety of related fields such as cybersecurity and cybercrime as well as corresponding law firms all over the world advising on local legal issues. We approach mandates with a global, solution-oriented and practical approach to deliver pragmatic and sustainable solutions.
Our clients are large and small companies in a variety of industries, including pharmaceuticals, biotechnology and medical devices, technology, consumer goods, luxury goods, food and beverages, transportation and logistics, automotive, insurance, financial institutions and chemicals.

www.privacylegal.ch

FABIAN PRIVACY LEGAL

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group